VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA APLIKOVANÉ INFORMATIKY

Implementace počítačové sítě

Implementation of computer network

Student: Miroslav Rod

Vedoucí bakalářské práce: Ing. Petr Rozehnal, Ph.D.

Ostrava 2011

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání bakalářské práce

Student:	**Miroslav Rod**
Studijní program:	B6209 Systémové inženýrství a informatika
Studijní obor:	6209R001 Aplikovaná informatika
Téma:	Implementace počítačové sítě
	Implementation of Computer Network

Zásady pro vypracování:

1. Úvod
2. Metodologická východiska a základní pojmy počítačových sítí
3. Analýza současného stavu ve firmě
4. Návrh rozšíření počítačové sítě
5. Zhodnocení navrhovaného řešení
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledku bakalářské práce
Přílohy

Seznam doporučené odborné literatury:

KÁLLAY, F.; PENIAK, P. *Počítačové sítě LAN/MAN/WAN a jejich aplikace.* 2. vyd. Praha: Grada Publishing, 2003. 356 s. ISBN 80-247-0545-1.
PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z.* 2. vyd. Brno: Computer Press, 2006. 430 s. ISBN 80-251-1278-0.
TANENBAUM, A. *Computer networks.* 4th ed. Upper Saddle River: Prentice Hall, 2003. 891 s. ISBN 0-13-166836-6.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Petr Rozehnal, Ph.D.**

Datum zadání: 26.11.2010

Datum odevzdání: 11.05.2011

Ing. Jan Ministr, Ph.D.	prof. Dr. Ing. Dana Dluhošová
vedoucí katedry	*děkanka fakulty*

Místopřísežně prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 2.5.2011 ……

Miroslav Rod

Obsah

1 Úvod

Počítač byl už od počátku velkým přínosem a usnadněním pro mnohé odvětví lidské činnosti. Postupem času se vypracoval až na označení osobní a setkáme se s nim v každé firmě, téměř na každém stole. Pro mnohé je už dnes nepředstavitelné, že by se bez něj měli obejít a denně za jeho obrazovkou stráví několik hodin. Propojování počítačů do počítačových sítí umožnilo posílat, sdílet informace nebo zařízení, které jsou v síti. V případě celosvětové sítě Internet můžeme tyto informace přenést téměř komukoliv, kdo má k této veřejné síti přístup.

Mnoho firem již dnes má připojení k internetu a využívá ho ke komunikaci se svými dodavateli či odběrateli, nebo si touto cestou hledá nové partnery. Pouze minimum firem vlastní jen jeden počítač, u kterého není zapotřebí sdílet data nebo zařízení, je proto ve většině firem nutné vytvořit aspoň jednoduchou síť pro sdílení například tiskáren nebo připojení k internetu.

V dnešní době tyto informační technologie usnadňují práci s informacemi, které jsou pro každou firmu velmi cenné a velmi důležité pro její vývoj a úspěch na trhu. Přesto mnoho firem po vytvoření počítačové sítě do ní neprovádí zásahy, dokud se něco nepokazí nebo síť již nesplňuje požadavky nového zařízení. V takovém případě jsou zásahy do sítě vykonávány pod časovým tlakem, a vzniká tak mnoho neuvážených výběrů komponent a počítačového vybavení. Proto by se informační technologie neměly stávat zanedbávanou součástí firemní infrastruktury, ale měly by se rozrůstat a zlepšovat s růstem společnosti.

Ve firemních počítačích je mnoho důležitých dat, které mají vysokou cenu, která stoupne v očích zaměstnanců nejvíce ve chvíli, kdy o ně přijdou nebo se poškodí. Proto by se tato data měla pravidelně zálohovat.

O veškeré počítačové vybavení by se měl někdo starat a udržovat ho aktualizované a maximálně provozu schopné dle možností firmy. U velkých firem již dnes bývá samozřejmostí, že mají své specializované úseky, které se této problematice věnují. U malých a středních firem si nemůžou dovolit mít vlastní specializovaný úsek, který by se staral o informační technologie, ale mnohdy se o tato zařízení stará někdo ze zaměstnanců, nebo si pro své vybavení najímají specializované firmy.

Cílem mé práce proto bude, zabývat se výběrem vhodně implementovatelných síťových zařízení do malé firmy.

2 Metodologická východiska a základní pojmy počítačových sítí

2.1 Uchovávání dat

Uchovávání dat je proces, kdy data ponecháváme na určitém nosiči, tak aby byla snadno vyhledatelná a čitelná. Existuje několik technologií pro zápis a čtení dat. Podle zvolené technologie paměťového média se také mění doba trvanlivosti těchto uložených dat.

2.1.1 Zálohování

Záloha je kopie dat uložená na jiném nosiči, nejlépe na jiném místě. Záloha je využita v případě ztráty, poškození nebo jiné nedostupnosti dat v případě jejich potřeby. Záloha je vytvářena buď v pravidelných, nebo nepravidelných časových intervalech. Zálohy se můžou provádět na různá média a s různou metodikou pro prováděný obsah dat [2].

Způsoby provádění záloh se u jednotlivých zálohovacích systémů liší. Následující rozdělení popisuje běžné metody a metody serverových systémů[2]:

- **Nestrukturovaná**

Tato záloha je nejjednodušší a je prováděna zkopírováním dat z disku na CD, DVD nebo USB flash disk.

- **Úplná + inkrementální**

Tento model zálohování spočívá ve vytvoření úplné zálohy všech dat. Posléze jsou vytvářeny inkrementální zálohy, při niž jsou zálohovány pouze data změněná od vytvoření úplné zálohy nebo poslední inkrementální. Obnova dat probíhá tak, že je nejprve využita úplná záloha a následně všechny inkrementální zálohy.

- **Úplná + rozdílová**

Toto zálohování vytváří nejprve úplnou zálohu jako předešlý model. Jednotlivé změny však nejsou ukládány do jednotlivých inkrementálních záloh, jak byly vytvářeny a následně zálohovány, ale vždy je vytvořena rozdílová záloha se změnami vytvořenými od vytvoření úplné zálohy. To v praxi znamená, že při obnově ze zálohy je zapotřebí nejprve použít úplnou zálohu a poté poslední rozdílovou zálohu, která obsahuje veškeré změny.

- **Zrcadlová + přírůstková**

Tento systém zálohy obsahuje zrcadlo, které vždy vytváří aktuální úplnou zálohu, kterou doplňuje o změny. To však vyžaduje vždy srovnání s aktuální zálohou, proto se nevyužívají optická média ale pevné disky.

- **Průběžná ochrana dat**

Tento způsob záloh je efektivnější než pouhé zrcadlení tím, že po každé změně zapisuje tyto změny do zálohy, nemaže však původní zálohy, což umožňuje zpětné vrácení souboru dat před změnou.

Média pro ukládání dat [8]:

- **Magnetická páska**

Jedno z nejpoužívanějších medií, které v dnešní době převyšuje svou rychlostí i pevné disky. Nevýhodou magnetických pásek je nákladnost na pořízení páskové jednotky. Na druhé straně je však nízká cena médií.

- **Pevný disk**

Poměr kapacity a ceny disku se čím dál zlepšuje, to dělá z pevných disků největšího konkurenta pro magnetické pásky. Díky jejich rozhraní nebo použití různých řadičů je jejich zakomponování velice levné.

- **NAS**

Označuje anglickou zkratku pro Network Attached Storage, což představuje pevný disk nebo pole pevných disků připojených do počítačové sítě. Takovéto zařízení může být jednoúčelové nebo server se speciálním softwarem, jehož úkolem je skladování dat.

- **Optický disk**

Výhodou optických disků je jejich cena. Představují je CD, DVD, DVD-RAM a Blu-ray disky. Optické disky nejsou vhodné pro dlouhodobou zálohu dat, z důvodu jejich mechanického poškození jako je pouhé poškrábání nebo zlomení, které zapříčiní jejich nečitelnost v optických mechanikách.

- **Vzdálená zálohovací služba**

V dnešní době, kdy je internet běžnou záležitostí se rozrůstají služby, které jsou tímto médiem poskytovány. Mezi nespočtem těchto služeb je i vzdálené zálohování. Toto řešení je výhodné k přesunu dat z naší blízkosti, čímž omezíme jejich možné zničení požárem či povodněmi nebo jinými povětrnostními vlivy. Na druhou stranu je to negativní vlastnost tohoto způsobu zálohování dat, protože tato data mohou být při přenosu napadena hackerem a samotný přenos může být pomalejší než u klasických paměťových médií.

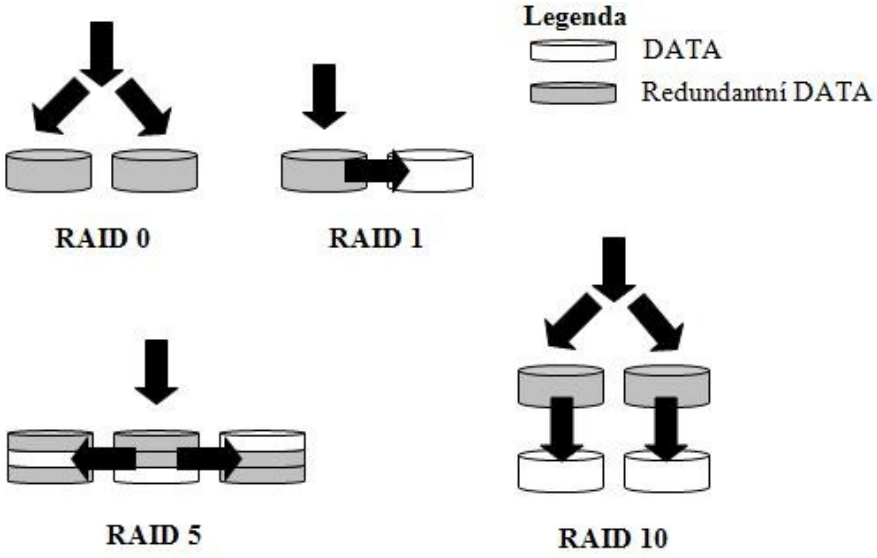
- **Ostatní paměťová média**

Dále se ještě pro krátkodobé zálohování používají různé flashové paměti jako jsou například USB flash disky nebo paměťové karty.

2.1.2 Diskové pole

Jde o skupinu disků, které navenek vypadají jako jeden disk. Takovéto pole disků si samo organizuje, na který disk se data uloží, případně ze kterého se přečtou, k tomu se používá některá z metod RAID. Disková pole se používají především pro zvýšení bezpečnosti dat, která je docílena redundancí dat. Redundance dat vzniká vytvořením kopie dat na druhý disk[2].

Obrázek 2.1.2-1: Metody zápisu dat pomoci RAID.



Zdroj: [2]

RAID 0

Data se rozdělí mezi několik disků. Tímto způsobem zvýšíme kapacitu, avšak nezvýšíme bezpečnost dat.

RAID 1

Data se při zápisu zapisují současně na více disků, obvykle na dva. Dochází k 100% redundanci dat. V případě poruchy jednoho disku, přebírá jeho funkci druhý disk.

RAID 5

Data jsou při zápisu rozdělována mezi disky. Redundantní data se rovnoměrně rozdělují mezi disky.

RAID 10

Data jsou rozdělena mezi několik disků jako v případě RAID 0, avšak tyto disky jsou ještě zrcadleny podle metodiky RAID1. Pro RAID10 je zapotřebí minimálně 4 disků.

2.2 Počítačové sítě

Počítačová síť je soustava vzájemně propojených počítačů a hardwarových prvků, které díky počítačové síti můžou mezi sebou sdílet a přenášet data, sdílet hardwarové prostředky a také umožňuje vzájemnou komunikaci hardwarových prvků na základě přístupových práv.

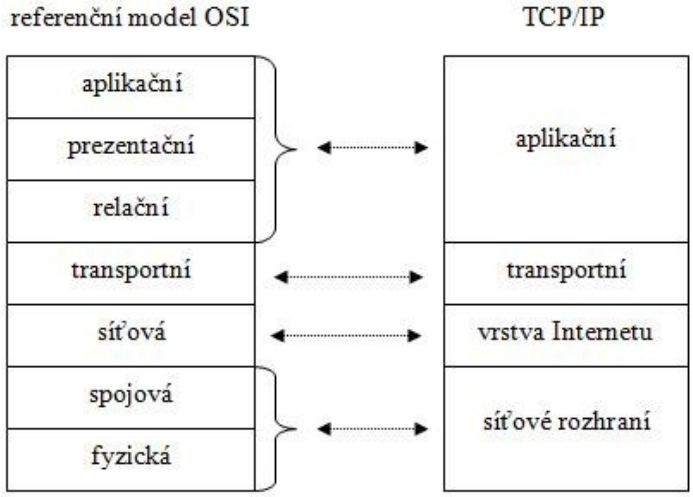
Počítačové sítě můžeme rozdělit dle rozlehlosti do tří kategorií LAN, MAN, WAN. Sítě LAN (Local area networks) jsou omezeny na jedno lokální místo například budovu nebo podnik.

Sítě WAN (Wide area networks) se označují za rozlehlé sítě. Tyto sítě se skládají z více vzájemně propojených sítí LAN. Jedná se například o síť mezi více městy, v rámci země či kontinentu až po celosvětovou síť Internet. Síť MAN (Metropolitan area network) je menší než WAN a větší než LAN. Jedná se o sítě v rámci měst [3].

2.2.1 Architektura TCP/IP

Tato architektura je skupinou protokolů, které jsou nejrozšířenější. Používají se v internetu, v sítích Novell i Microsoft. Obrázek 2.2.1-1 zobrazuje souvislost této architektury s referenčním modelem OSI. Data jsou zapouzdřována do hlaviček, jak postupně procházejí jednotlivými vrstvami architektury [4].

Obrázek 2.2.1-1



Zdroj: [4]

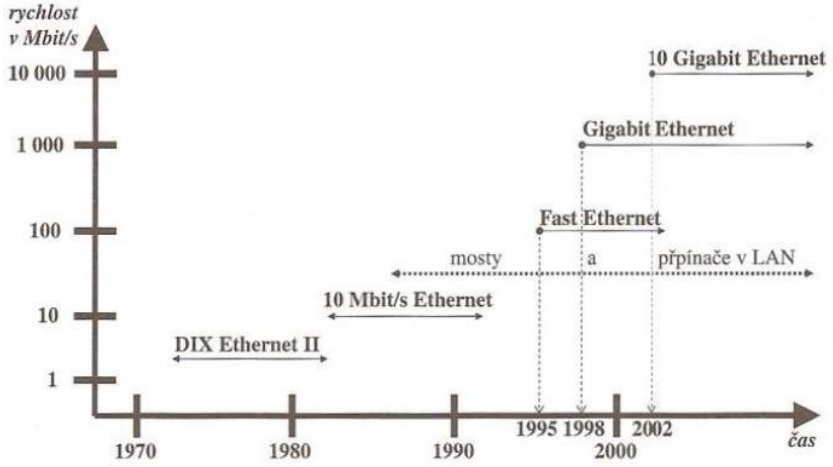
2.2.1.1 Vrstva síťového rozhraní

Nejnižší vrstva, která umožňuje přístup k fyzickému přenosovému médiu, je specifická pro každou síť (Ethernet, Token ring, FDDI). Tato vrstva přidá hlavičku, která obsahuje zdrojovou a cílovou MAC adresu[4].

802.3 Ethernet

Tato technologie má za sebou již více než třicetiletou úspěšnou historii, která tkví v jednoduchosti protokolu, což umožňuje jednoduchou instalaci a údržbu sítě s nižšími náklady. Proto se tato technologie stala nejrozšířenější technologií pro výstavbu LAN sítí. S postupem času se navyšovala rychlost přenášených dat, a tak vznikaly jednotlivé varianty.

Obrázek 2.2.1.1-1: Vývoj Ethernetu.



Zdroj: [4]

U sítí Ethernet je vysílání stanic prováděnou metodou CSMA/CD, která využívá ke sdílené sběrnici metodu mnohonásobného přístupu prostřednictvím naslouchání nosné a s detekcí kolizí (Carrier Sense Multiple Access with Collision Detection). Tato metoda funguje tak, že stanice, která chce přenést data, sleduje, co se děje na přenosovém médiu. V případě, že na médiu neprobíhá přenos, začne přenášet. Může se však stát, že začnou přenášet dvě stanice najednou a dojde ke kolizi z důvodu sdíleného média. V tom případě se vyšle signál označující kolizi tzv. jam. Stanice si stanoví náhodnou dobu čekání, a poté zkusí přenos dat znovu. Ke kolizím dochází z důvodu přenosového zpoždění, které vzniká tím, že signál se teprve blíží a není detekován stanicí, která chce taky vysílat. Největší zpoždění nastává u nejvzdálenějších stanic. V případě, že na přenosovém médiu probíhá přenos, stanice počká a zkusí znovu detekovat přenos dokud se neuvolní přenosové médium a stanice nepřenese data [4].

Tak, jak se zvyšovala rychlost přenesených dat ve variantách Ethernetu, měnila se pro jednotlivé varianty i kabeláž.

U drátových sítí se dnes používají dva typy kabelů a to kroucená dvojlinka a optický kabel. Třetím vodičem je koaxiální kabel, ale z důvodu jeho morálního zastarání a nahrazování kroucenou dvojlinkou jej nebudu popisovat.

- **Kroucená dvojlinka**

Kroucená dvojlinka je nejrozšířenější vodič v sítích LAN. Tento vodič se skládá z 8 metalických vodičů tvořících 4 páry. Vzájemné rušení vodičů je ochráněno tím, že páry

jsou navzájem zkrouceny a dále vzniklé zkroucené 4 páry jsou mezi sebou taktéž zkrouceny, tím se minimalizuje vzájemné rušení vodičů.

Kabely, s nimiž se setkáme nejčastěji, mají označení cat. 5 nebo cat. 5e. Toto označení slouží pro rozlišení vnitřní konstrukce kabelu, která podle označení udává přenosové rychlosti [4].

Tabulka 2.2.1.1-1: Standardy kroucené dvojlinky.

Standard	Označení	Rychlost přenosu	Konektor	Šířka pásma
100 Base – T	Kategorie 5	100 Mb/s	RJ – 45	100 MHz
1 000 Base – T	Kategorie 5e	1 000 Mb/s	RJ – 45	125 MHz
1 000 Base – TX	Kategorie 6	1 000 Mb/s	RJ – 45	250 MHz
1 000 Base – TX2	Kategorie 7	1 000 Mb/s	GC45, TERA	600 MHz

Zdroj: [2]

Strukturovaná kabeláž je optimální hardwarové uspořádání sítě, při kterém je využita hvězdicová topologie. Každá zásuvka je připojena kroucenou dvojlinkou do propojovacího panelu v rozvaděčové skříni. Ve skříni je kromě propojovacího panelu ještě switch a ostatní aktivní síťové prvky, které jsou napojeny k propojovacímu panelu, a tím umožňují velkou variabilitu připojitelných zařízení. Například může být do rozvaděčové skříně přidána telefonní ústředna, pak stačí kabel z propojovacího panelu napojit k telefonní ústředně a příslušná zásuvka se dá využít pro telefon. Tato modulárnost strukturované kabeláže umožňuje snazší údržbu a identifikaci oprav, včetně snadného přechodu na jiné komunikační prvky bez nutnosti investic do rozvodů [2].

- **Optický kabel**

Data v optických kabelech jsou přenášena za pomocí světelných impulzů ve světlovodivých vláknech. Vlákna jsou vložena do vrstvy sekundární ochrany, která by měla zabránit mikroohybům a makroohybům kabelu, při kterém by mohlo dojít k útlumu světelného paprsku v kabelu. V jednom kabelu bývají minimálně dvě vlákna - pro každý směr přenosu jedno. Dále je kabel složen z konstrukční vrstvy, která zvyšuje jeho pevnost. Poslední vrstvou je plastové vnější krytí.

Optické kabely můžeme rozdělit podle konstrukce optického vlákna na mnohovidové a jednovidové.

U mnohovidových jsou optické vlastnosti horší díky lomům vedeného světelného paprsku, který se rozvětví na několik částí (vidů), které dorazí na konec vlákna v různém čase

a tím dojde ke zkreslení signálu. Tyto kabely jsou levnější a hodí se spíše do sítí LAN, kde se jedná o stovky metrů přenosu.

Jednovidové kabely jsou přesnější, protože jimi prochází pouze jeden paprsek, což umožňuje použít tyto kabely na vzdálenosti desítky kilometrů. Díky jejich kvalitě jsou tyto kabely dražší a v sítích LAN se s nimi setkáme výjimečně [4].

Bezdrátové sítě

Bezdrátové sítě používají jako přenosové médium vzduch, proto u takto vytvářených sítí nemusíme řešit, kudy bude signál veden. Signál je ovlivněn vysílacím výkonem zařízení a jeho antény. Bezdrátové propojení se dělí do licenčního a bezlicenčního pásma. Do bezlicenčního pásma spadá nejpoužívanější technologie pro tvorbu bezdrátových lokálních sítí - technologie WiFi.

IEEE 802.11

Je standard organizace IEEE pro lokální bezdrátové sítě. Původním záměrem tohoto standardu bylo propojení přenosných zařízení do lokálních sítí. S postupem času se tato technologie začala využívat pro připojení k internetu pomocí takzvaných hotspotů. V dnešní době je tento standard znám pod pojmem WiFi. Takovéto označení mohou mít pouze zařízení, která splňují testovací kritéria WiFi Alliance. Zařízení, která jsou nositeli WiFi loga, zaručují propojitelnost těchto zařízení mezi sebou, využívají-li stejný standard. Dnes jsou WiFi standardem opatřovány téměř všechny přenosné počítače a některé mobilní telefony. WiFi je provozováno v bezlicenčním pásmu, což způsobuje silné zarušení, jenž má negativní vliv na fungovaní bezdrátové sítě[6].

Tabulka 2.2.1.1-2: Standardy IEEE 802.11.

Standard	Pásmo	Maximální rychlost
IEEE 802.11a	5 GHz	54 Mbit/s
IEEE 802.11b	2,4 GHz	11 Mbit/s
IEEE 802.11g	2,4 GHz	54 Mbit/s
IEEE 802.11n	2,4 nebo 5 GHz	600 Mbit/s

Zdroj: [4]

U bezdrátových sítí se můžeme setkat s dvěmi způsoby komunikace[6]:

- **Ad-hoc mód**

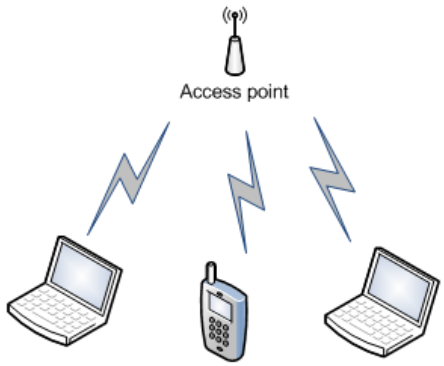
V této síti se spojují dva klienti a utvářejí peer-to-peer síť, která je velmi podobná propojení dvou počítačů za pomocí křížené kroucené dvojlinky. Pro stavbu této sítě je zapotřebí, pouze aby oba propojované počítače měly bezdrátovou síťovou kartu pracující ve stejném pásmu s možností práce v zapojení Ad-hoc.

Obrázek 2.2.1.1-2: Ad-hoc zapojení.

- **Infrastrukturní mód**

K tomuto zapojení je zapotřebí, aby byl v síti alespoň jeden aktivní prvek. V bezdrátových sítích se takovýmto zařízením říká přístupový bod, přezdívaný jako AP (zkratka z anglického Access Point). Toto AP slouží jako vysílající bod, ke kterému se připojují jednotlivé stanice. AP je identifikováno pomocí SSID, tj. názvu dané sítě. Několik sítí může být stejně pojmenováno a bezdrátový klient se přepojuje k jednotlivým AP v závislosti na síle signálu. To umožňuje klientovi se pohybovat v prostoru sítě.

Obrázek 2.2.1.1-3: Připojení pomoci Access point.



Zabezpečení sítě

U drátových sítí jsou data bezpečně vedena kabelem a pokud se někdo nedostane ke kabelu a nepřipojí se kabelem do sítě, jsou data v bezpečí. U bezdrátových sítí je médium vzduch a kdokoliv by měl dostatečný signál na připojení se k síti, mohl by odposlouchávat

přenášená data, což by ohrozilo bezpečnost celé sítě, proto se využívají následující možnosti zabezpečení bezdrátových sítí[6]:

- **Zablokování vysílání SSID**

Toto řešení porušuje standard, ale je nejjednodušší řešení, jak zabezpečit síť. Zablokováním vysílání broadcastu s SSID znemožníme viditelnost AP a tím docílíme, že běžným uživatelům se tato síť nezobrazí v dostupných bezdrátových sítích vyhledávaných na počítači. SSID lze však odposlouchat pokud se někdo začne připojovat k AP, protože toto připojování je v otevřené podobě.

- **Kontrola MAC adres**

Přístupový bod má v sobě uloženu tabulku MAC adres klientů, podle které je umožněno připojení klientů. V případě, že útočník bude mít MAC adresu, která odpovídá některé z tabulky, může se vydávat za věrohodného klienta.

- **802.1X**

Toto zabezpečení vyžaduje na straně přístupového bodu autentizaci pomocí protokolu IEEE 802.1X. Pro ověření je používán na straně klienta program, který nazýváme prosebník, kterému přístupový bod zprostředkuje komunikaci s třetí stranou, která ověření provede. Za pomoci 802.1X lze odstranit nedostatky zabezpečení pomocí WEP klíčů.

- **WEP**

Šifrování pomocí statických WEP klíčů, které jsou zadány jak na klientově straně, tak i na AP. Díky nedostatku v protokolu je velice jednoduché se k WEP klíči dostat. Stačí odchytnout určité rámce a jejich analýzou dostaneme klíč. V současnosti pro získání WEP klíče existuje řada programů.

- **WPA**

Toto šifrování využívá WEP klíče, které jsou dynamicky bezpečným způsobem měněny. To umožňuje zpětnou komptabilitu a možnost vybavit starší zařízení WPA šifrováním. Autentizace přístupu do WPA sítě je prováděno pomocí PSK (Pre-Shared Key – obě strany používají stejnou dostatečně dlouhou heslovou frázi) nebo RADIUS server (ověřování přihlašovacím jménem a heslem).

- **WPA2**

Je novější a kvalitnější než jeho předchůdce WPA, avšak pro jeho využívání je zapotřebí většího výpočetního výkonu. Z tohoto důvodu není možné tuto technologii implementovat do starších zařízení.

Šíření radiového signálu

Pro WiFi antény platí pravidlo, že by mezi nimi měla být přímá viditelnost. Tento fakt však nestačí pro chod takového spojení. Tento rádiový přenos signálu narušují buď přírodní faktory nebo lidská činnost. Nejdůležitější vliv na rušení rádiového signálu mají jiná zařízení ve stejném frekvenčním pásmu. Mezi technologie, které fungují ve stejném frekvenčním pásmu patří Breeze Net, Bluetooth, mikrovlnné trouby, bezdrátové telefony a v neposlední řadě jiné bezdrátové sítě WiFi.

V přímé viditelnosti venkovního použití WiFi spojení můžou bránit buď budovy, stromy nebo terénní nerovnosti. Při nepřízni počasí, jako je husté sněžení, bouřka či mlha se signál může dočasně snížit.

Při interiérovém propojení jsou překážkou příčky budovy, které dle použitého materiálu signál odstíní, nebo propustí [6].

2.2.1.2 Síťová vrstva

Vrstva, která zajišťuje síťovou adresaci, směřování a předávání datagramů. Tato vrstva přidá hlavičku, která obsahuje zdrojovou a cílovou IP adresu[4].

2.2.1.3 Transportní vrstva

Tato vrstva je implementována do koncových zařízení a umožňuje přizpůsobit chování sítě potřebám aplikace. Transportní služby poskytuje protokolem TCP nebo UDP[4].

2.2.1.4 Aplikační vrstva

Vrstva aplikací, které používají síť k přenosu dat. Pro identifikaci těchto síťových přenosů jednotlivých aplikací se jim přiřazují tzv. porty, což jsou domluvená číselná označení aplikací[4].

2.2.2 Model ISO/OSI

Model ISO/OSI stanovuje pravidla pro přenos dat v sítích a mezi nimi. Tuto komunikaci rozděluje do sedmi vrstev. Každá vrstva má svou funkci.

Aplikační vrstva zprostředkovává síťové služby uživatelům v jejich programech. **Prezentační vrstva** se stará o sjednocení formy přenášených dat, která může dále šifrovat nebo komprimovat. **Relační vrstva** navazuje a ukončuje navázané spojení. **Transportní vrstva** se stará o rozdělení přenášených dat na pakety a při opačném prostupu vrstev o jejich složení. **Síťová vrstva** zajišťuje spojení mezi počítači nebo sítěmi, které nemají přímé spojení. Tím se stará o volbu trasy přenášených dat. **Linková vrstva** provádí přenos dat po fyzickém médiu a pracuje s fyzickými adresami zařízení, u kterých určuje, co má být s daty provedeno. **Fyzická vrstva** popisuje vlastnosti přenosového média a definuje logickou jedničku a nulu[3].

2.3 Aktivní prvky sítě

Samotná kabeláž pro přenos dat v síti nestačí, je zapotřebí dalších prvků, které s daty aktivně pracují tak, že například umožňují rozbočení sítě, nebo propojení sítí na dvou odlišných přenosových médiích. Na trhu se mnohdy setkáme s jedním typem hardware, který slučuje více aktivních prvků do jednoho zařízení. Například router kombinovaný se čtyř portovým switchem, který poskytuje předěl mezi celosvětovou sítí Internet a lokální sítí hvězdicové topologie [2].

Zesilovač (repeater)

Nejjednodušší aktivní prvek sítě, který pouze zesiluje procházející signál. Tento prvek je vybaven dvěma stejnými konektory. Jeden slouží pro příjem signálu a z druhého vystupuje zesílený signál. Toto se využívá u kabelů, které jsou natolik dlouhé, že by na jejich konci nebyl dostatečně silný signál.

Převodník (transceiver)

Převodník je velmi podobný zesilovači, taktéž signál zesiluje. Navíc převodník převádí jeden typ kabelu na jiný.

Rozbočovač (hub)

Rozbočovač je předchůdcem dnešního zařízení switch. Jeho úkolem bylo rozvětvení sítě do hvězdicové topologie. Jeho nevýhodou bylo, že data posílal všem větvím sítě, čímž zatěžoval síť.

Most (bridge)

Tento prvek provádí aktivní směrování dat rozvětvené sítě na základě filtrace přenášených paketů. Tato technologie bývá velmi často integrována do rozbočovačů, což snižuje zatížení sítě, protože se posílají data jen adresátům.

Switch

Switch je dnes centrem všech hvězdicových topologií, kde větví sítě. Pracuje na principu filtrování paketů mezi zdířkami, což mu umožňuje obsluhovat více spojení najednou.

Směřovač (router)

Prvek, který shromažďuje informace o síti a na jejich základě vybírá nejkratší cestu posílaných dat. V sítích LAN se s ním moc nesetkáme, typickým použitím směřovače je při připojování k sítí Internet.

Brána (gateway)

Slouží k připojování lokálních sítí na cizí prostředí.

2.4 Virtuální privátní sítě

Virtuální privátní sítě (VPN) nejsou specifické svou technologií, ale zaměřují se na využití veřejných infrastruktur, kterou může představovat například internet, veřejná IP síť. VPN vytváří logickou síť v rámci veřejné sítě, při zachování charakteru privátní sítě.

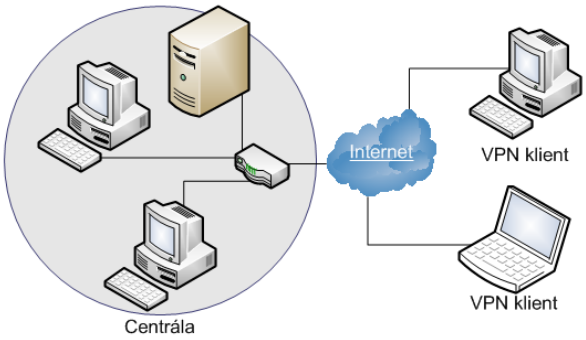
Komunikace probíhá tak, že data odesilatele projdou VPN branou, umístěnou na hranici mezi privátní a veřejnou sítí. Data jsou přenesena veřejnou sítí k další VPN bráně, která data zpracuje pro využití v privátní síti [4].

Rozlišujeme dva typy VPN sítí[9]:

Remote-access poskytuje uživatelům pracujícím doma nebo na cestách spojení se vzdáleným přístupem se serverem v organizaci za pomoci využití veřejné sítě. Tento model se nejvíce uplatňuje v organizacích, které mají centrální sídlo a jejich zaměstnanci jsou často

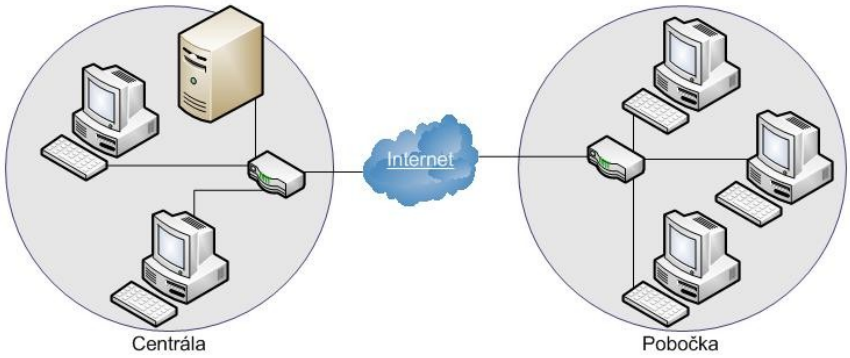
na cestách nebo pracují z domu. Tato metoda funguje na principu připojení klienta VPN k VPN bráně, která je nejčastěji umístěna v centrále firmy. Takto využívanou komunikaci zobrazuje obrázek 2.4-1.

Obrázek 2.4-1



Site-to-Site architekturu můžeme rozdělit na dva druhy: Intranet a Extranet. Intranet slouží k propojení mezi jednotlivými pobočkami organizace, které se nacházejí z geografického hlediska v různých lokalitách a za pomoci VPN tyto lokální sítě můžeme spojit. Extranet slouží k vytvoření spojení mezi lokálními sítěmi důvěryhodných obchodních partnerů. Takto vytvářené spojení znázorňuje obrázek 2.4-2.

Obrázek 2.4-2



VPN sítě mohou vznikat za pomocí softwaru, který je implemenován do serveru na síti, nebo může být implementován výrobcem v aktivním prvku (router, firewall).

Zabezpečení přenosu dat ve VPN sítích je několik. Níže uvedená tabulka 2.4-1 obsahuje technologie zabezpečení a typy spojení, které je možné u těchto zabezpečení využít.

Tabulka 2.4-1

Typ technologie	Vrstva OSI modelu	Site-to-Site	Remote-Access
MPLS	2/3	Ano	ne
PPTP	2	Ne	ano
L2TP	2	Ne	ano
IPSec	3	Ano	ano
SSL/TLS	4	Ne	ano
SSH	4	Ne	ano

Zdroj: [9]

2.5 Rozhodování

Rozhodování je proces poznávání jednotlivých variant, směřující ke konečné volbě varianty. Výsledkem rozhodování je tedy rozhodnutí, které může vyvolat určité chování nebo postoj dle vybrané varianty. Výslednou variantu vybírá jednotlivec nebo skupina lidí tak, aby bylo dosaženo nejlepšího naplnění cílů. Rozhodovací proces je nejčastěji využit při plánování. Kvalita výsledného rozhodnutí proto může značně ovlivnit budoucnost.

Teorie uplatnitelné při rozhodování [1]:

Teorie užitku – hodnotíme varianty podle zvolených kritérií

Sociálně-psychologické teorie – zaměřuje se na subjekt a jeho chování

Kvalitativně orientované – aplikujeme matematické modely a metody jako je třeba teorie her nebo operační analýza

Teorie rozhodování v organizacích – zohledňuje omezené schopnosti organizace rozhodovat

Základní postup rozhodovacího procesu [1]:

1. Identifikace situací, které potřebují řešení. Pro tyto situace se snažíme nashromáždit co nejvíce informací, které pomohou formulovat problém.
2. Formulace problému tak, aby byly stanoveny příčiny vzniku problému a následné stanovení cílů pro řešení.
3. Stanovení kritérií, která budou měřítkem pro porovnání variant.
4. Stanovení vhodných variant, která vedou k vyřešení problému.
5. Stanovení důsledků jednotlivých variant na základě stanovených kritérií.

6. Vyhodnocení variant a stanovení optimální varianty nebo preferenčního uspořádání variant.
7. Uvedení vybrané varianty do praxe.
8. Porovnání odchýlení reálného fungování varianty od očekávaného fungování varianty s případnými nápravnými opatřeními nebo přepracováním cílů, které nebyly stanoveny realisticky.

Rozhodovací analýza

Rozhodovací analýza je heuristická metoda vhodná pro řešení složitých rozhodovacích problémů a je ji možné využít tam, kde je potřeba učinit kvalifikované rozhodnutí. Tato metoda spočívá ve vyjádření preference variant, které srovnává dle užitnosti a rizika variant. Umožňuje tak určit nejlepší vhodné řešení. Metoda se svou strukturou podobá základnímu postupu rozhodovacího procesu. Vlastní aplikaci rozhodovacího procesu můžeme rozdělit do sedmí fází [7]:

1. Vymezení problému a stanovení cílů. Je základem rozhodovací analýzy, bez něj by naše výsledné rozhodnutí nemělo smysl.
2. Rozbor informací a podkladů. V této druhé fázi se jedná o poznávání problému se sběrem informací, které poskytnou podklady pro stanovení variant, stanovení kritérií hodnocení variant a nepříznivých důsledků jednotlivých variant.
3. Stanovení variant. Na základě cílů a vymezeného problému stanovíme reálné varianty, které směřují k vyřešení problému.
4. Stanovení kritérií. Cílem této fáze je stanovit vhodný soubor kriterií, která budou vhodně hodnotit důsledek jednotlivých variant z pohledu stanovených cílů.
5. Hodnocení a srovnání variant. Z předchozích čtyř fází rozhodovací analýzy můžeme vytvořit neformální přehled potřebných údajů nebo rozhodovací matici. Rozhodovací matice vyobrazuje preference rozhodovacího subjektu k jednotlivým variantám podle jednotlivých kritérií. Výsledkem v této fázi by mělo být prosté nebo vážené ohodnocení užitnosti variant.
6. Zjištění nepříznivých důsledků. Výběr varianty by měl vést ke zdokonalení současného stavu. Tato změna však může mít i nepříznivý vliv. Proto je vhodné vybrat variantu, která zohledňuje nejmenší nepříznivé vlivy. K tomu můžeme použít slovní popis nebo rozhodovací matici.

7. Volba nejvhodnější varianty. Toto rozhodnutí by mělo vybrat nejvhodnější variantu, která nejlépe splňuje soubor kriterií s nejmenšími nepříznivými důsledky pro stanovený cíl.

3 Analýza současného stavu

Firma REZ servis s.r.o. se zabývá zejména pronájmem stavebních strojů, přepravy stavebního materiálu, provádění staveb, jejich změn a odstraňování. Firma dále funguje jako konsignační sklad sypkých materiálů. Společnost má nyní 6 správních zaměstnanců včetně ředitele a 15 technických pracovníků.

Společnost sídlí ve dvou budovách, které jsou mezi sebou vzdáleny cca 1,5 km vzdušnou čarou. První budova je administrativní a je zde umístěna většina počítačové techniky. V druhé budově se nacházejí techničtí pracovníci. Obě budovy jsou nyní zvlášť napojeny k síti Internet a to od dvou různých místních poskytovatelů internetu za pomoci WiFi technologie. Tito poskytovatelé umístili na střechy objektů svá WiFi zařízení, která však zůstala v jejich vlastnictví a správě. Poskytovatelé u svých připojeních k internetu poskytli veřejnou IP adresu. Tato WiFi zařízení jsou napojena za pomoci UTP do počítačové sítě.

Parametry internetu administrativní budovy:

Poskytovatel: PODA a.s.
Tarif: Garant 5000 kbps
Max. rychlost: 5000 kbps/5000 kbps (downstream/upstream)
FUP: bez omezení
Cena: 2 880,- Kč/měsíc

Parametry internetu napojení technické budovy:

Poskytovatel: TechCom s.r.o.
Tarif: FIRMA_start
Max. rychlost: 4096 kbps/1228 kbps (downstream/upstream)
FUP: bez omezení
Cena: 1 178,- Kč/měsíc

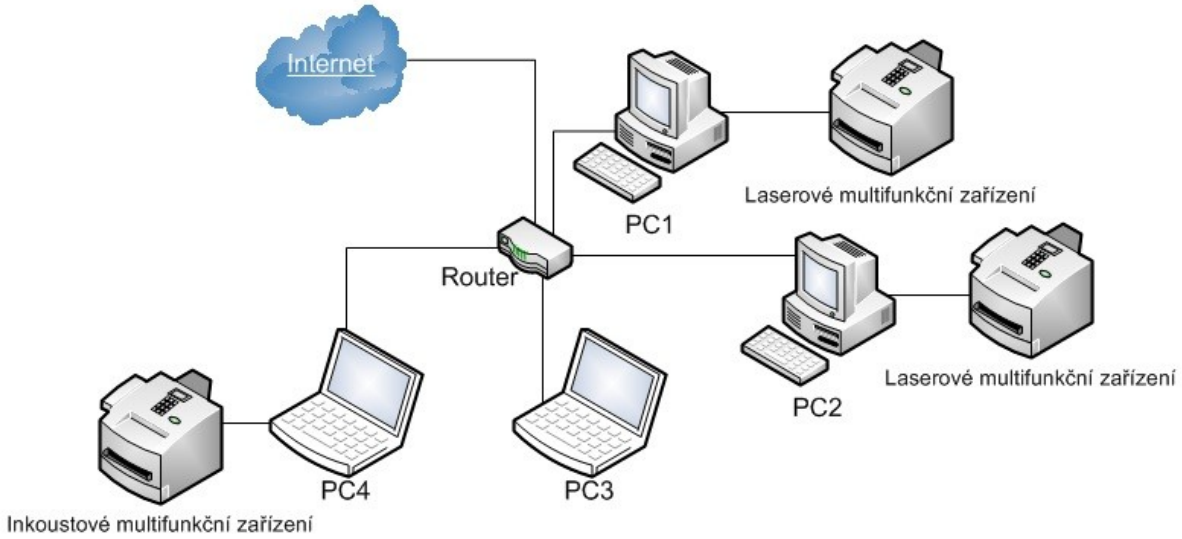
V administrativní budově se nyní nachází dva stolní počítače, dva notebooky, dvě velké laserové multifunkční tiskárny a jedna inkoustová multifunkční tiskárna. Tyto počítače jsou využívány k práci s elektronickou poštou, s ekonomickým softwarem, k tvorbě návrhů stavebních projektů a k běžné kancelářské činnosti.

Všechny počítače jsou vybaveny síťovou kartou pro kroucenou dvojlinku ať už přímo na základní desce počítače nebo přídavnou kartou pro PCI slot. Notebooky jsou navíc

vybaveny bezdrátovým adapterem pro příjem standardu 802.11g. Tento bezdrátový adaptér však není zatím možné využít v síti administrativní budovy, jelikož jsou počítače připojeny do routeru značky TP-LINK, model TL-R402M, který disponuje 4 portovým rozbočovačem, který umožňuje maximální přenosovou rychlost 100 Mbps. Kabeláž je tvořena kroucenou dvojlinkou kategorie 5e. Dvě velké laserové multifunkční tiskárny jsou připojeny do sítě za pomoci stolních počítačů, na kterých jsou sdíleny pro zpřístupnění ostatním počítačům v síti. Zbylá tiskárna je napojena přímo k počítači a není sdílena v síti.

Síť je nyní využívána pro sdílení tiskáren, internetu a pro využití síťové verze účetního programu WinDUO. WinDUO je nainstalován na počítači PC1, který sdílí složku s účetním programem všem počítačům v administrativní budově. Tento počítač funguje jako server pro tento účetní software.

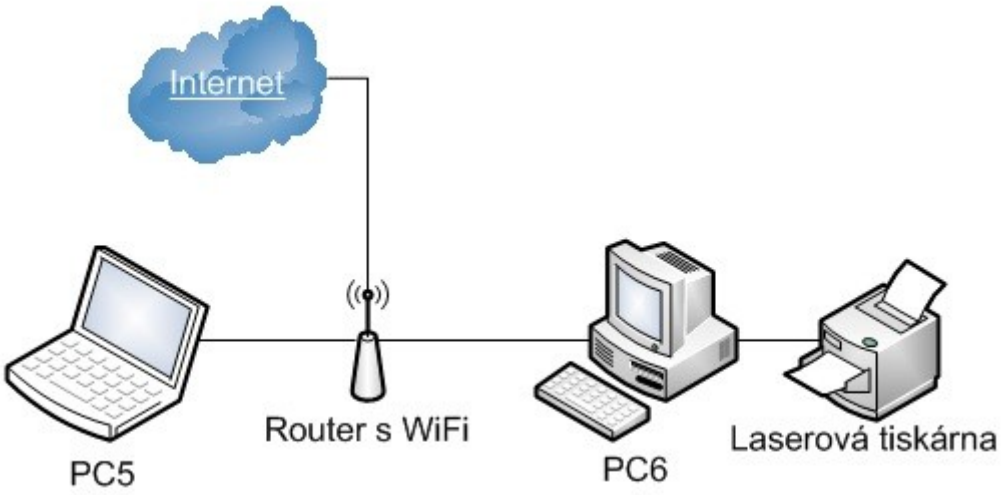
Obrázek 3-1: Schéma sítě administrativní budovy.



V druhé budově jsou soustředěni techničtí pracovníci. V této budově je jeden stolní počítač a jeden notebook. Tyto počítače jsou připojeny k WiFi routeru značky TP-LINK, model TL-WR542G. Notebook je připojen do sítě za pomocí vestavěného bezdrátového adapteru WiFi standardu 802.11g. Stolní počítač je připojen do sítě pomocí síťové karty, která je umístěna na základní desce a kabelem kategorie 5e. Také je zde zatím jedna laserová tiskárna, která je připojena ke stolnímu počítači a pro potřeby pracovníka používajícího notebook je tato tiskárna sdílena. Počítače slouží ke komunikaci s dodavateli přes síť Internet a k zjišťování informací na internetu. Na jednom z počítačů běží databáze s veškerým výdejem štěrkového materiálu. Tato databáze slouží k reportování lomům a jako podklad pro vystavování faktur. Pro některé své činnosti je zapotřebí získání nebo zadání dat

do ekonomického softwaru WinDUO, což momentálně znamená pro zaměstnance přesun do administrativní budovy nebo telefonát s účetní.

Obrázek 3-2: Schéma sítě technické budovy.



Počítačové vybavení není starší více než 5 let a na všech počítačích je nainstalován Microsoft Windows XP. Toto vybavení zatím společnosti stačí a není potřeba jej vyměnit za novější, proto jej nebudu v práci řešit.

Veškeré počítače svá data ukládají na lokální pevný disk a každý z pracovníků si zálohuje svá data dle svého uvážení. Většinou zálohují na flash disky v nepravidelných intervalech. Pro správce sítě je pak při jakékoliv ztrátě dat obtížné obnovit data ze zálohy, pokud už nějaké zálohy vůbec existují.

Společnost si přeje navrhnout spojení dvou sítí jednotlivých budov z důvodu snazšího sdílení souborů na síti a taktéž využití síťové verze ekonomického programu WinDUO i v technické budově. Nynější stav zálohování dat je velmi chaotický a velké množství dat není dnes zálohováno. Proto je zapotřebí navrhnout vhodný zálohovací systém, který by nespoléhal na spuštění obsluhou počítače, ale aby veškeré zálohování probíhalo automaticky. Tento systém musí zároveň umožňovat snadný přístup k zálohovaným datům a jejich obnově.

Veškeré přidávané komponenty by měly být vhodně implementovány s ohledem na stávající vybavení společnosti tak, aby byl pokud možno zachován stávající hardware a software.

Po konzultaci s ředitelem společnosti jsme stanovili finanční limit pro spojení budov a zálohování dat okolo 15 000,- Kč. Přáním ředitele také je, aby se příliš nezvyšovaly náklady na samotný provoz sítě.

4 Návrh rozšíření počítačové sítě

4.1 Propojení dvou budov

V současné době se nabízí mnoho řešení, jak lze propojit dvě vzdálenější místa. Tyto možnosti bychom mohli rozdělit mezi kabelové a bezdrátové.

Kabelové spojení na delší vzdálenosti však skýtá mnoho úskalí, jelikož se musí vést buď průvěsy (zavěšení mezi budovami nebo zavěšení na stožáry veřejného osvětlení apod.) nebo pod povrchem země. Kabelové spojení je velmi nákladné a navíc se při jeho provádění setkáváme s řadou legislativních a vlastnických problémů. Proto kabelové propojení je výhodné pouze pokud je takováto realizace prováděna na kratší vzdálenosti (do 100 m) a nejlépe přes vlastní pozemek. V našem případě je vzdálenost mezi budovami poměrně velká (cca 1,5 km) a pozemky jsou ve vlastnictví cizího subjektu. Proto kabelové spojení nedoporučuji.

V našem případě je vhodnější pro propojení budov na takto velkou vzdálenost bezdrátová technologie. Existuje varianta licenčního a bezlicenčního pásma. Licenční pásmo nabízí nejlepší možnou kvalitu spojení, avšak za příliš vysokou cenu, která překračuje stanovený finanční limit. U bezlicenčního pásma žádné poplatky nejsou, a proto je vhodné tuto možnost využít. Pro propojení by tato technologie měla být dostačující. Neobáváme se velkého zarušení a cenově je pro nás dostupná.

Z předchozích odstavců vyplývá, že lepší východisko pro propojení dvou budov na větší vzdálenost a přes více pozemků je použití bezdrátové technologie. Z finančních důvodů je lepším řešením bezlicenční pásmo. V dnešní době je nejrozšířenější technologií bezdrátového přenosu využívajících bezlicenčí pásmo technologie standardu IEEE 802.11. Pro snazší implementaci prvků doporučuji využít certifikovaných zařízení s označením WiFi, které musí splňovat parametry WiFi alliance pro vzájemnou komunikaci a využívají ke komunikaci standard IEEE 802.11.

Další variantou, jak propojit druhou budovu, je využití veřejných sítí. Jako veřejnou síť můžeme využít celosvětové sítě Internet, ke které jsou obě budovy připojeny, a tak lze využít technologie VPN tunelů.

Za vhodné pro spojení považuji dvě poslední uvedené varianty, WiFi a VPN tunel. V případě varianty WiFi spojení je však nutné brát v potaz vzdálenost a možné vlivy, které ovlivní sílu signálu, což bude mít dopad na kvalitu takto vytvořeného spojení. V případě VPN

tunelu bude síť záviset na internetovém připojení, což při současném trendu snižování ceny a zvyšování rychlosti připojení by neměl být problém vytvořit kvalitní spojení. Proto se v práci budu zabývat pouze těmito dvěmi možnostmi, jak sloučit stávající sítě do jedné.

4.1.1 WiFi varianta

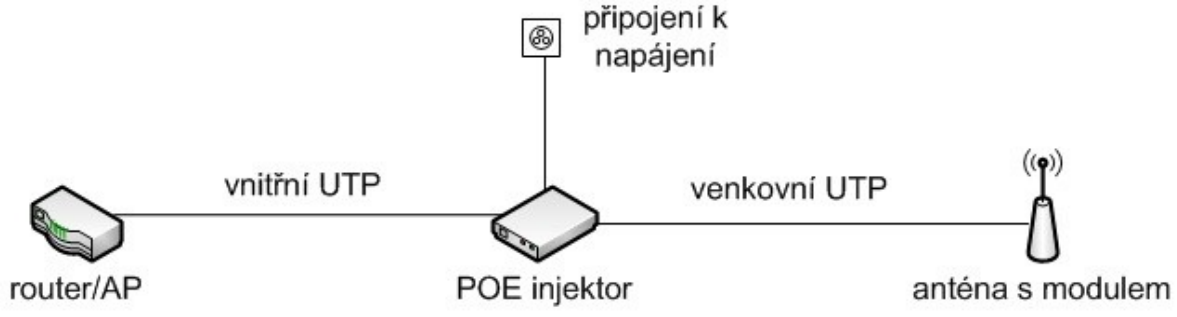
Nároky na hardware

K WiFi propojení je zapotřebí dvou zařízení, které podporují provozní mód bridge, někdy je udáván mód point-to-point, který umožní spojení sítí mezi oběmi budovami a sloučí obě lokální sítě do jedné. Na trhu najdeme i taková zařízení, která umožňují na místo point-to-point technologie technologii point-to-multipoint. Tuto technologii můžeme také použít, ale nevyužijeme její možnosti fungování v síti naplno. Na trhu je dnes mnoho zařízení, která mód point-to-point nebo point-to-multipoint podporují.

Pro snazší implementaci takovýchto zařízení se dnes dají na trhu koupit kompletní venkovní zařízení, která mají v sobě anténu a hardwarový modul, který má klasický síťový výstup, jenž umožňuje napájení po UTP, což umožní takovéto zařízení umístit na stožár nebo na objekt, a tak veškeré napájení a správu těchto WiFi pojítek můžeme provádět z místnosti uvnitř budovy. Antény obou zařízení by měly být směrové, aby jejich signál byl co nejsilnější ve vysílaném směru a nedocházelo tak ke zbytečnému vysílání signálu z antény ve směru, kde jej není třeba.

Jelikož budeme instalovat anténu ven a rozhodli jsme se, že budeme mít anténu včetně hardwarového modulu do kterého přivedeme UTP s daty, měli bychom počítat s použitím venkovního UTP kabelu. Toto UTP nám postačí na propojení mezi venkovním hardwarovým modulem a uvnitř umístěným POE injektorem. Od tohoto injektoru nám postačí obyčejný UTP kabel.

Obrázek 4.1.1-1: Zapojení POE injektoru s vhodnými UTP kabely.



WiFi nabízí dvě frekvenční pásma a to 2,4 GHz a 5 GHz. Pásmo 2,4 GHz se objevuje nejčastěji v noteboocích a jiných zařízeních, které využívají napojení k přístupovému bodu nebo vytvoření spojení mezi stanicemi. Síť v pásmu 2,4 GHz je již v technické budově provozována a mohlo by tak docházet k rušení těchto signálů, proto využijeme pro spojení budov pásmo 5 GHz. Přivedený internet do budov je proveden WiFi zařízeními, která jsou taktéž na frekvenci 5 GHz. Tyto antény jsou však směrové, a nevytvářejí proto velkou hrozbu. Dalším opatřením proti rušení těchto antén je vytvoření komunikace našeho bezdrátového mostu na jiném kanálu, než na kterém komunikují stávající pojítka internetových poskytovatelů.

Zařízení s nastaveným módem point-to-point využívá pro zabránění připojení neautorizovaného zařízení MAC adresu. Pro bezdrátovou komunikaci je důležitá bezpečnost přenášených dat dána úrovní šifrování, proto navrhuji použít zařízení, které umožňuje šifrování WPA2.

Vhodný hardware

Tabulka 4.1.1-1 ukazuje výběr pěti zařízení, která jsou momentálně dostupná na trhu a splňují naše požadavky pro vytvoření WiFi mostu pro spojení sítí obou budov firmy. Tabulka 4.1.1-2 pak popisuje parametry těchto vybraných zařízení.

Tabulka 4.1.1-1

	Zařízení	Cena bez DPH
A	Compex WPP543A-7C	1 843,- Kč
B	Kozumi AIR FORCE ONE 5	1 516,- Kč
C	Mikrotik RB SXT 5HnD	1 591,- Kč
D	OvisLink AirLive AirMax5	1 320,- Kč
E	UBNT NanoBridge M5	1 807,- Kč

Ceny odpovídají stavu k 9.4.2011 internetového obchodu wifi.aspa.cz.

Tabulka 4.1.1-2

	WiFi standard	Teoretická přenosová rychlost	Zisk antény
A	802.11a/b/g/n	108 Mbps	13 dBi
B	802.11n	300 Mbps	14 dBi
C	802.11a/n	300 Mbps	16 dBi
D	802.11a	108 Mbps	14 dBi
E	802.11n	300 Mbps	22 dBi

Informace o jednotlivých zařízeních čerpám z produktových listů, které jsem našel na internetových stránkách jednotlivých výrobců. Tyto produktové listy přikládám v příloze bakalářské práce.

Výběr hardware

Vybraná pětice zařízení splňuje veškeré požadavky pro WiFi most. Zařízení jsou dle požadavku vybavena LAN portem pro standardní konektor RJ45 s napájením po UTP za pomoci POE injektoru. Zařízení se od sebe liší parametry antén a použitým standardem pro přenos dat. Všechna zařízení obsahují webové administrativní rozhraní pro nastavování zařízení.

Pro naše bezdrátové propojení je anténa důležitým prvkem zařízení. U antény bychom se měli zaměřit na co největší zisk a na co nejmenší vyzařovací úhel. Některé z vybraných prvků nabízejí možnost připojení externí antény, která umožní zlepšení parametru celkového WiFi pojítka. To však navýší cenu a degraduje kompletní zařízení s hardware jednotkou a anténou pouze na obyčejnou hardware jednotku s připojenou externí anténou. U hardwarového modulu zařízení je důležitým parametrem standard, který jednotka využívá pro komunikaci. Tento standard nám umožní určit teoretickou přenosovou rychlost, která udává nejvyšší možnou rychlost přenášených dat mezi zařízeními. Tato rychlost by měla být pro náš účel co nejvyšší. Jelikož jsou ceny jednotlivých zařízení téměř stejné a rozdíl mezi nejdražším a nejlevnějším zařízením se pohybuje pouze okolo 500,- Kč, není tento parametr příliš důležitý.

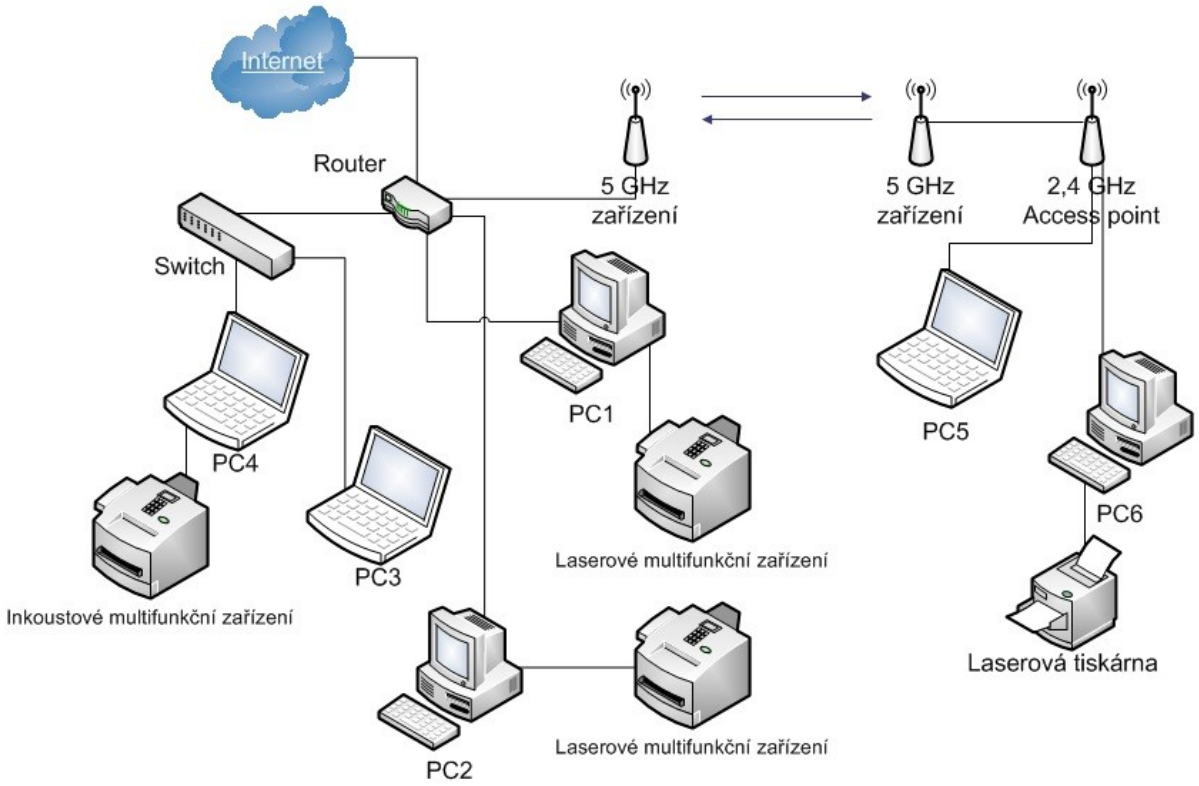
Po zhodnocení parametrů zařízení, jsem vyhodnotil, že nejvhodnějším zařízením z pětice navrhovaných je zařízení společnosti Ubiquiti Networks model NanoBridge M5 (v tabulce 4.1.1-1 označeno jako C). Toto zařízení má nejlepší parametry antény a pro přenos dat využívá standard 802.11n, jenž umožňuje vysokou přenosovou rychlost.

Implementace prvků

Síť administrativní budovy se změní tak, že do sítě přibude switch, protože současný router má již zaplněnu kapacitu portů. Pro tento účel postačí běžný switch s pěti porty. Do tohoto rozbočovače se připojí dva počítače. WiFi pojítko napojíme přímo do routeru. Toto zařízení bychom měli umístit na střechu tak, aby bylo co nejvíce nasměrováno na druhé WiFi zařízení na technické budově. V technické budově bude přidáno taktéž 5 GHz zařízení, které by mělo být umístěno na nejvyšší místo budovy tak, aby obě tato zařízení na sebe měla

dobrou viditelnost. Následně se na UTP kabel vystupující z tohoto zařízení připojí WiFi access point, který však nebude mít zapnutou službu DHCP serveru, jelikož jediným prvkem, který toto bude umožňovat a do celé sítě přidělovat, bude router v administrativní budově. V technické budově můžeme stávajícímu internetovému poskytovateli vypovědět odebírání služby, jelikož nám u nově vytvořené sítě postačuje jedno internetové připojení. Rozhodl jsem se využít internetového připojení administrativní budovy, protože nabízí lepší parametry a kvalitu této poskytované služby. Obrázek 4.1.1-2 znázorňuje změny v síti při použití WiFi mostu pro spojení obou budov.

Obrázek 4.1.1-2



Cenová kalkulace

Náklady na vybudování WiFi varianty jsou uvedeny v tabulce 4.1.1-3. V této tabulce jsou použity ceny hardware z internetového obchodu wifi.aspa.cz aktuální k datu 9.4.2011. Spotřeba venkovního UTP kabelu je odhadnuta na 20 m. Tato délka se při samotné instalaci může změnit. Instalaci a nastavení hardware bude provádět místní firma LWT JaryNet s.r.o., která má se zařízeními společnosti UBNT zkušenosti z vlastní sítě. Firma odhaduje práci včetně pomocného instalačního materiálu na 2 000,- Kč. Výsledná délka použitého kabelu bude fakturována dle skutečné spotřeby. Odhadovaný náklad na WiFi spojení je 6 162,- Kč.

Tabulka 4.1.1-3

Položka	Množství	Cena za jednotku	Cena
UBNT NanoBridge M5	2 ks	1 807,- Kč	3 614,- Kč
Switch Zyxel ES-105	1 ks	268,- Kč	268,- Kč
Venkovní UTP kabel	20 m	11,- Kč	220,- Kč
Konektor RJ45	4 ks	4,- Kč	16,- Kč
Patch kabel UTP, cat. 5e, 2m	2 ks	22,- Kč	44,- Kč
Instalace a nastavení	-	2 000,- Kč	2 000,- Kč
Celkové náklady			6 162,- Kč

Roční náklady při využití WiFi varianty znázorňuje tabulka 4.1.1-4. Rozdíl po spojení sítí odpovídá ušetřeným nákladům za připojení k internetu technické budovy. Objevil se však náklad v podobě údržby této bezdrátové sítě. Tento náklad je odhadován na 1 000,- Kč/rok a je v něm obsažen 2x výjezd technika pro zkontrolování funkčnosti sítě. Tento náklad se však v reálném fungování může lišit podle toho, jak moc bude bezdrátová síť poruchová.

Tabulka 4.1.1-4

Položka	Náklady před změnou sítě/rok	Náklady po změně sítě/rok
Internet administrativní budovy	34 560,- Kč	34 560,- Kč
Internet technické budovy	14 136,- Kč	-
Správa WiFi sítě	-	1 000,- Kč
Celkové náklady	48 696,- Kč	35 560,- Kč

4.1.2 VPN varianta

Nároky na hardware

V případě nasazení VPN do provozu existují dva způsoby zavedení. Nasazení speciálního hardwaru, který bude vytvářet VPN tunely. Druhou možností je implementovat software na počítač, který se stane vstupní bránou a bezpečnostním firewall jak do sítě Internet, tak pro jednotlivé tunely VPN. Obě varianty jsou cenově rozdílné a mají své specifické požadavky pro uspořádání prvků sítě. Jelikož firma nemá dva přebytečné starší počítače, které by se daly předělat na vstupní brány, jeví se jako výhodnější varianta, ta při které se zapojí dva routery s možností vytvářet VPN spojení. Z pohledu spotřeby elektrické energie a pořizovacích nákladů je tato varianta ekonomičtější, proto další postup výběru se bude týkat routerů s funkcí VPN.

Pro takto vytvářené spojení bude třeba speciálního hardware pro vytvoření VPN tunelu typu Site-to-Site, který umožní propojení dvou lokálních sítí jednotlivých budov. Toto zařízení by mělo být schopno vytvářet alespoň 1 VPN tunel. Dále by mělo podporovat zabezpečovací protokol IPSec, který je sice složitější, ale bezpečnější než jiné a umožňuje vytvoření tunelu mezi jednotlivými zařízeními i přímo s počítačem mimo podnikovou síť.

Vhodný hardware

Na trhu je nyní několik vhodných zařízení pro navrhované použití v cenové relaci do 6 000,-Kč. Tato zařízení jsou v tabulce 4.1.2-1

Tabulka 4.1.2-1

Zařízení	Počet IPSec tunelů	Porty	Rychlost síťových portů	Cena
Mikrotik RB750G	neomezeně	5xLAN/WAN	10/100/1 000 Mbps	1 260,- Kč
D-Link DI-804HV	40	4xLAN 1xWAN RS-232	10/100 Mbps 10/100 Mbps	1 528,- Kč
Zyxel ZyWALL 5	10	4xLAN 1xWAN RS-232 PCMCIA	10/100 Mbps 10/100 Mbps	5 645,- Kč

Ceny v tabulce odpovídají stavu k 9.4.2011 internetového obchodu wifi.aspa.cz.

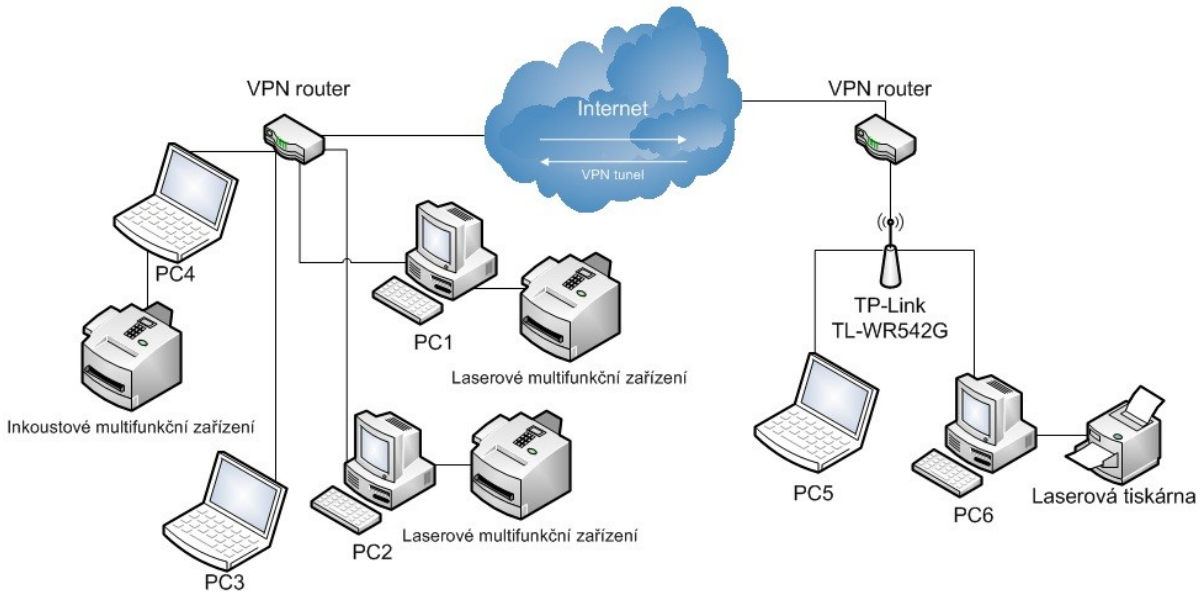
Výběr hardware

Z trojice zařízení, která podporují tvorbu VPN tunelů vybočuje z řady zařízení společnosti Mikrotik model RB750G. Tento model je vybaven jako jediný gigabitovými porty, které se sice momentálně ve firemní síti nevyužijí naplno, avšak při budoucí obměně počítačů najdou své uplatnění. Toto zařízení má velké možnosti nastavování díky RouterOS, což je grafický operační systém na bázi Linuxu. Toto zařízení je proto spíše omezeno hardwarově než softwarově. Zbylá dvě zařízení mají podobná vybavení. Zařízení společnosti Zyxel oproti zařízení společnosti D-Link nabízí větší možnosti co se týče záložního připojení k internetu, a to za pomoci PCMCIA karty, do které můžeme vsunout přídavné karty mobilních operátorů pro připojení k internetu. Toto zařízení je však příliš drahé. Funkci náhradního připojení k internetu společnost nevyužije a zvyšovala by tím náklady pro provoz spojení. Proto doporučuji zvolit zařízení společnosti Mikrotik, které nabízí nejlepší cenu a jehož hardwarové parametry jsou na velice dobré úrovni.

Implementace prvků

Síť administrativní budovy se změní nahrazením stávajícího routeru, který nahradí nový router s VPN funkcí. Tento router se nastaví tak, aby vytvářel VPN tunel skrz veřejnou síť Internet na nově přidané zařízení v technické budově. V technické budově se připojí VPN router tak, že se do něj přivede kabel s internetem a stávající WiFi router, který poskytuje připojení do sítě. Na WiFi routeru je třeba zapnout funkci VPN pass-trough. Tato funkce umožní propouštění VPN tunelu na zařízení připojená k WiFi routeru. Na obrázku 4.1.2-1 je zobrazeno zapojení s využitím VPN technologie.

Obrázek 4.1.2-1



Cenová kalkulace

Náklady na vybudování VPN varianty jsou rozepsány v tabulce 4.1.2-2. Ceny hardware odpovídají internetovému obchodu wifi.aspa.cz odpovídající k datu 9.4.2011. Nastavení zařízení svěříme firmě LWT JaryNet s.r.o. Tato firma má proškolené pracovníky pro nastavování zařízení od společnosti Mikrotik a má s těmito zařízeními dlouholetou zkušenost. Odhadovaná cena pro vybudování VPN varianty činí 3 764,- Kč.

Tabulka 4.1.2-2

Položka	Množství	Cena za jednotku	Cena
Mikrotik RB750G	2 ks	1 260,- Kč	2 520,- Kč
Patch kabel UTP, cat. 5e, 2m	2 ks	22,- Kč	44,- Kč
Instalace a nastavení	-	1 200,- Kč	1 200,- Kč
Celkové náklady			3 764,- Kč

Roční provozní náklady při VPN variantě rozepisuje tabulka 4.1.2-3. Při VPN variantě nám zůstala obě připojení k internetu. Přibyl náklad na správu sítě, který jsem odhadem vyčíslil na 500,- Kč. Nepředpokládám nějakou složitou údržbu tohoto spojení, ale v průběhu životnosti se můžou vyskytnout různé anomálie sítě. Proto počítám alespoň s jedním výjezdem technika ročně.

Tabulka 4.1.2-3

Položka	Náklady před změnou sítě/rok	Náklady po změně sítě/rok
Internet administrativní budovy	34 560,- Kč	34 560,- Kč
Internet technické budovy	14 136,- Kč	14 136,- Kč
Správa sítě	-	500,- Kč
Celkové náklady	48 696,- Kč	49 196,- Kč

4.1.3 Porovnání WiFi a VPN varianty

Obě varianty splní svůj účel, propojení budov. Varianty však mají své výhody i nevýhody, které se mohou časem projevit. Vyhodnocením výhod a nevýhod lze jednu variantu upřednostnit před druhou.

Výhody WiFi varianty spočívají v možnosti využití jednoho připojení k internetu a tím snížit náklady na připojení. Internetové připojení pak můžeme sdílet v rámci vytvořené sítě.

U VPN propojení je zapotřebí, aby obě budovy měly své napojení k internetu, jelikož tuto veřejnou síť využívají k přenosu dat. Momentálně však firma platí obě připojení k internetu, a tak si myslím, že kdyby jim vadila výše poplatků za připojení k internetu, je vždy možnost najít jiného cenově dostupnějšího poskytovatele internetu. VPN varianta nabízí možnost vytvořit zabezpečené připojení pracovníků do firemní sítě tak, aby mohli pracovat v síti, i když budou fyzicky jinde než v budovách společnosti. VPN zařízení nabízí i při přestěhování administrativních nebo technických pracovníků do jiné budovy možnost opětovného vytvoření spojení přes internet, který předpokládám si nechá společnost do jiných prostor zavést, jelikož jej využívá pro svou komunikaci a hledání informací. K tomu postačí pouze upravit nastavení VPN routerů, aby vytvářely zabezpečený tunel mezi sebou.

U WiFi mostu toto nemusí být vždy možné kvůli zarušení, větší vzdálenosti nebo nemožnosti přímé viditelnosti mezi oběmi WiFi anténami. Také z odstupem času se může stát, že dojde k většímu zarušení nebo nemožnosti přímé viditelnosti mezi WiFi anténami, což

může mít za následek, že WiFi varianta přestane fungovat a její další provoz již nebude možný.

Z výše uvedených kladů a záporů variant bych více doporučil VPN variantu. Obě varianty ještě podrobně porovnám pomoci metody rozhodovací analýzy.

Stanovení variant:

Varianta 1 (V1) – Propojení za pomocí WiFi mostu.

Varianta 2 (V2) – Propojení za pomoci VPN tunelu.

Kritéria pro stanovení optimální varianty řešení:

Spolehlivost spojení – požadavek na funkčnost vytvořeného propojení budov. Toto spojení by mělo být co nejlepší.

Další využití spojení – jaké jsou další možnosti takto vytvořeného spojení budov. Popřípadě možnosti využití zařízení v budoucnu. Jelikož na řešení vynakládáme finanční prostředky, očekáváme co nejlepší využitelnost do budoucna.

Cena vytvoření spojení – tato cena by měla obsahovat náklady spojené s vytvořením spojení. Tato cena by měla být co nejmenší.

Náklady na chod sítě – tyto náklady se týkají položek běžného fungování sítě během jednoho roku. Výši nákladů na chod sítě očekáváme co nejmenší.

Varianty nebudu porovnávat z pohledu rizika, neboť je na zařízení poskytována stejná záruční lhůta a riziko použití již zohledňuje kritérium spolehlivosti spojení.

Tabulka 4.1.3-1: Charakteristika variant.

	Charakteristika	Jednotka	V1	V2
K1	Spolehlivost spojení	-	střední	nejlepší
K2	Další využití spojení	-	horší	nejlepší
K3	Cena vytvoření spojení	Kč	6 162	3 764
K4	Náklady na chod sítě	Kč	35 560	49 196

Tabulka 4.1.3-2: Matice prostých užitností.

	Charakteristika	V1	V2
K1	Spolehlivost spojení	85	100
K2	Další využití spojení	70	100
K3	Cena vytvoření spojení	85	100
K4	Náklady na chod sítě	100	80

Tabulka 4.1.3-3: Párové porovnání kritérií.

Tabulka 4.1.3-4: Stanovení vah jednotlivých kritérií.

	Četnost	Pořadí	Váha
K1	3	1	4
K2	2	2	3
K3	1	3	2
K4	0	4	1

Tabulka 4.1.3-5: Matice vážených užitností.

	Charakteristika	Váha	V1	V2	Maximum
K1	Spolehlivost spojení	4	340	400	400
K2	Další využití spojení	3	210	300	300
K3	Cena vytvoření spojení	2	170	200	200
K4	Náklady na chod sítě	1	100	80	100
	Celková užitnost		820	980	1 000
U	Relativní užitnost		82%	98%	100%

Z hlediska užitku se jako nejlepší varianta jeví varianta 2, VPN tunel. Tato metoda potvrdila mou volbu vycházející z výhod a nevýhod obou variant.

4.2 Zálohování dat

Při větším počtu počítačů vzniká problém, jak zálohovat data z jednotlivých stanic, jelikož data jsou ukládána na lokální disky jednotlivých stanic. Administrátor může obejít všechny stanice a na každé stanici vytvořit zálohu pro daný počítač na vybrané zálohovací médium, to je však zdrojově náročné a neefektivní. Je výhodnější zvolit zálohovací postup tak, aby se zálohovaná data shromažďovala na jeden centrální počítač (server), a poté se přesunula na vybrané médium. Jelikož sítě obou budov společnosti by měly být propojeny, můžeme zálohovat data po síti i z druhé budovy. Zálohování bych soustředil do administrativní budovy, jelikož je zde umístěna většina počítačů a větší množství dat pro zálohu.

Pro navržený postup zálohování s centrálním bodem můžeme využít již stávající počítač (PC1). Tento počítač je navržen jako server, ale neobsahuje serverový operační systém. Firemní síť proto funguje na hierarchii peer-to-peer a není tak možné optimálně zpřístupnit tyto data. Toto by se dalo vyřešit doinstalováním specializovaného software, který by umožňoval zpřístupnění dat z ostatních počítačů. Takto nashromážděná data je nutné přenést mimo tento počítač a společnost z důvodu zvýšení bezpečnosti zálohovaných dat. K tomuto účelu bych doporučil externí harddisk, který by se k PC1 připojil pomoci USB 2.0 a data by se na něj nakopírovala. Tato varianta předpokládá spolupráci správce sítě.

Druhou variantou je, že by se na tomto počítači vytvořily složky, které by byly sdíleny v síti a klienti jednotlivých stanic by k nim měli přístup a kopírovali by do těchto složek důležitá data určena k záloze. Tento postup však není automatický a vyžaduje určitou interakci ze strany uživatele počítače. Proto tento neautomatický postup nedoporučuji.

Jelikož se na stanici PC1 denně pracuje a jsou zde vytvářena data, která by bylo vhodné ochránit před ztrátou, doporučuji i tento počítač vynechat pro soustředění dat z jednotlivých stanic a raději přidat další zařízení. Toto zařízení by mělo úkol shromažďovat data z jednotlivých stanic, což by mělo za úkol ochránit data jednotlivých počítačů před ztrátou nebo poškozením dat jednotlivých stanic. Zařízení, které tyto služby dokáže poskytovat je NAS server.

Z předchozích odstavců vidíme, že možností jak zálohovat firemní data je několik a jako nejvhodnější bych doporučil poslední rozebíranou variantu, a to obohacení firemní sítě o NAS server. Toto zařízení je vhodné pro vytváření kopií dat z počítačů firmy a předcházet tak ztrátu dat při znehodnocení dat jednotlivých stanic. Tento postup ale není příliš vhodný při

ochraně dat před přírodními vlivy jako je oheň či voda nebo před lidským faktorem, jakým může být krádež hardware společnosti. Proto doporučuji ještě tento NAS server pravidelně zálohovat na externí disk, který se po zkopírování dat přenese mimo budovy společnosti. Tímto by zálohovací mechanismus měl vytvořit maximální ochranu dat společnosti.

Nároky na zálohovací hardware

Na trhu můžeme koupit kompletní zařízení, u kterého stačí osadit pevné disky do zařízení dle požadované kapacity, a zařízení může po svém nastavení plně sloužit. Druhou možností je složit si svůj vlastní NAS server a nainstalovat na něj vhodný operační systém. Pro využití v REZ servisu bych zvolil již kompletní zařízení, protože u kompletního zařízení kupujeme ucelený produkt s jednotnou uživatelskou podporou a zárukou. U serveru vlastní produkce je složitější jakákoliv změna a vyžaduje odbornou pomoc (nejlépe přímo konstruktéra, který tento server zná).

Požadavky na NAS server pro účel zálohování by měly být specifické tím, že by NAS server měl obsahovat dvě pozice pro pevný disk o velikosti 3,5" s rozhraním SATA. Tyto pozice osadíme dvěmi stejnými disky a u těchto disků budeme od zařízení požadovat metodu ukládání RAID 1. Touto metodou zabráníme ztrátám dat při poruše jednoho z disků. Minimální kapacita osaditelného disku by měla být alespoň 500 gigabyte. Což znamená minimální celkovou kapacitu NAS serveru alespoň 1 terabyte po osazení obou disků. Server by měl obsahovat softwarovou funkci pro zálohování dat z jednotlivých stanic v síti. Jelikož firma na svých počítačích využívá operační systém Windows XP, mělo by být zařízení kompatibilní s tímto operačním systémem. Pro výhled do budoucna by bylo samozřejmě vhodné, aby podporoval i novější a nyní prodávané operační systémy. Také by zařízení mělo být osazeno alespoň jedním USB portem standardu 2.0 pro vytváření záloh zařízení na externí harddisk.

Pro NAS server je potřeba vybrat vhodné dva disky, které by měly kapacitu 500 gigabyte. Tuto kapacitu jsem stanovil na základě momentálního datového vytížení stanic a očekávaného přírůstku dat. Dle požadavku na NAS server by měl disk mít velikost 3,5" s rozhraním SATA. Disky by měly mít co nejnižší spotřebu elektrické energie. Od tohoto parametru se odvíjí požadavek na nižší výkon otáček ploten a to okolo 5 400 otáček/minutu.

Externí disk pro vytvoření kopie dat z NAS server by měl mít kapacitu 500 gigabyte, aby bylo možné přemístit data z NAS serveru mimo budovu společnosti. Tento disk by měl být připojitelný k rozhraní USB 2.0 které je požadavkem i u NAS serveru. Novější standard

3.0 bude sice přínosem ale zatím jej nebude možné využít naplno, jelikož se tento standard zatím neosazuje do těchto serverů. Velikost disku by postačovala pro přenášení dat 3,5", ale dnes není na trhu v této kapacitě téměř žádné zařízení, proto bude výběr specifikován pro 2,5" externí disky. Tyto disky mají tu výhodu, že jsou napájeny pomocí USB sběrnice, a proto odpadá nutnost připojovat je přímo k elektrické síti. NAS servery by měly být schopny tyto 2,5" disky napájet.

Vhodný zálohovací hardware

Na základě požadovaných parametrů NAS serverů jsem vybral tři zařízení, která jsou uvedena v tabulce 4.2-1. Tato zařízení jsou si velmi podobná a příliš se od sebe neliší. Tyto servery nabízejí spoustu funkcí mimo požadovaných. Vybral jsem novější modely, které nabízejí lepší hardwarové parametry než jejich předchůdci, kteří se nyní doprodávají.

Tabulka 4.2-1

	Zařízení	Cena
A	D-Link DNS-325	4 555,- Kč
B	QNAP TS-210 Turbo NAS	4 555,- Kč
C	Synology DS211j Disc Station	4 570,- Kč

Tabulka 4.2-2: Parametry vybraných NAS serveru.

	Frekvence procesoru	Velikost operační paměti	Spotřeba elektrické energie
A	výrobce neuvádí	výrobce neuvádí	10,45 W hibernace, 21,04 W provoz
B	800 MHz	256 MB	60 W provoz
C	1,2 GHz	128 MB	10 W hibernace, 25 W provoz

Disky, které budou osazeny v NAS serveru jsem vybral dle stanovených kriterií a uvedl jsem do tabulky 4.2-3. V tabulce jsou zastoupeny disky od jednotlivých největších výrobců pevných disků.

Tabulka 4.2-3

	Zařízení	Cena
D	Samsung EcoGreen F2 3,5" 500GB HD502HI	862,- Kč
E	Seagate Pipeline HD 3,5" 500GB ST3500312CS	922,- Kč
F	Western Digital Caviar Green WD5000AADS 3,5" 500GB	914,- Kč

Tabulka 4.2-4: Parametry vybraných pevných disků.

	Přístupová doba	Cache paměť	Spotřeba el. energie
D	8,9 ms	16 MB	2,9 W v klidu, 5,1 W při zátěži
E	< 14 ms	8 MB	3,4 W při zátěži
F	8,9 ms	32 MB	3,7 W v klidu, 6 W při zátěži

U externích disků jsem taktéž vytvořil výběr dle stanovených kriterií. Do tabulky 4.2-5 vhodných disků jsem dosadil disky největších výrobců. Parametrově se disky liší pouze v použitém standardu USB portu. Zařízení společnosti Samsung a Western Digital nabízí USB 3.0. Zařízení společnosti Seagate obsahuje pouze USB 2.0, ale díky možnosti vyměnitelné sběrnice za jinou, je možné vyměnit sběrnici a využívat jej se standardem USB 3.0. Na disk společnosti Samsung je poskytnuta 36 měsíců dlouhá záruční doba, u zbylých dvou je to pouze 24 měsíců.

Tabulka 4.2-5

Zařízení	Cena
Samsung S2 Portable 500GB černý USB 3.0	1 544,- Kč
Seagate FreeAgent GoFlex 500GB černý	1 717,- Kč
Western Digital Passport Essential 500GB černý USB 3.0	1 865,- Kč

Veškeré ceny a parametry uvedených zařízení jsou čerpány z internetového obchodu ALFA COMPUTER a.s. k datu 12.4.2011. V příloze jsou přiloženy produktové listy NAS serverů.

Výběr vhodného hardware

Veškerý vybraný hardware splňuje požadavky. V případě samostatného NAS serveru vybočuje dle zvolených parametrů zařízení od společnosti Synology, které má nejvyšší takt procesoru při srovnatelné spotřebě elektrické energie, jako zařízení od společnosti D-Link. Zařízení od společnosti D-Link ale neuvádí takt procesoru ani operační paměť. Zařízení od společnosti Synology nabízí sice menší operační paměť než u zařízení společnosti QNAP, ale dokáže hospodárněji odebírat elektrickou energii. Proto doporučuji použít zařízení společnosti Synology, model DS211j Disc Station.

Disk, který budeme osazovat do NAS serveru, bych zvolil od společnosti Western Digital Caviar Green WD5000AADS 3,5" 500GB. Tento disk nabízí srovnatelnou přístupovou dobu jako disk společnosti Samsung. Oproti Samsungu má zařízení od Western Digital dvojnásobnou cach paměť. Co se týče odběru elektrické energie, tak tento vybraný

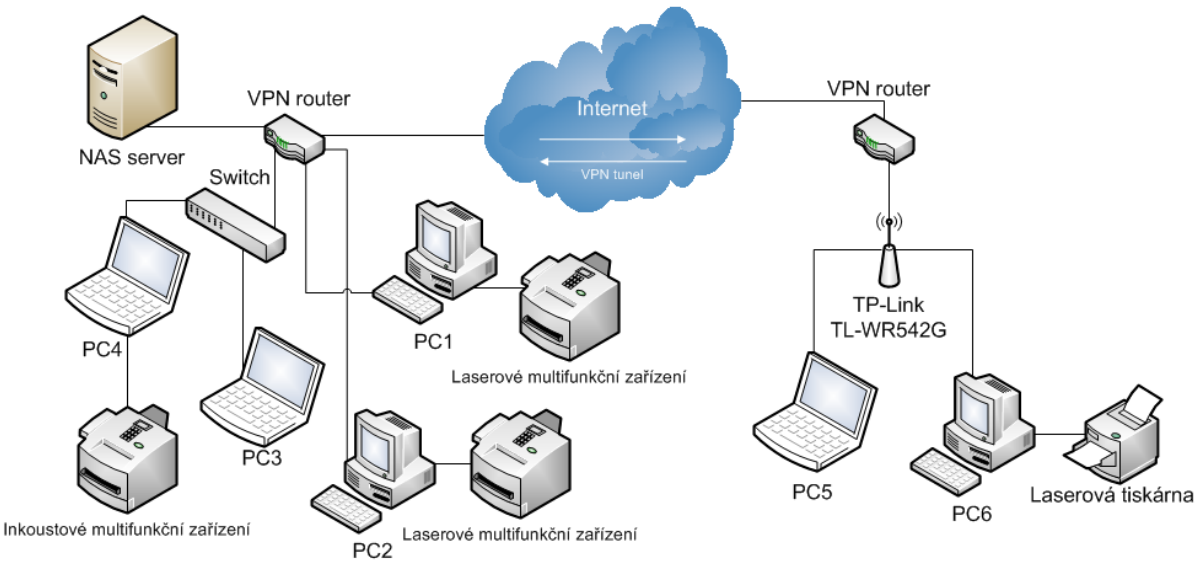
disk trochu ztrácí při srovnání se zbylými dvěmi disky. Disk společnosti Seagate se vyznačuje pouze hospodárnou spotřebou elektrické energie, což pro jeho zvolení nestačí.

Externí disk bych zvolil od společnosti Samsung, model S2 Portable 500GB černý USB 3.0, který jako jediný nabízí 36 měsíců záruční dobu a nejnižší nabízenou cenu z trojice vybraných.

Implementace zálohovacích prvků

Pro zapojení NAS serveru do sítě využijeme UTP kabel, který je součástí balení. Jelikož navrhujeme VPN routery do sítě budeme již počítat s touto změnou. Do sítě by proto měl být připojen switch, který umožní napojení dalších prvků do sítě z důvodu již plných portů VPN routeru. Jelikož vybraný VPN router obsahuje gigabytové porty, vybral jsem switch, který má 5 gigabytových portů. Zapojení do sítě zobrazuje obrázek 4.2-1. Do NAS serveru vložíme dva disky od společnosti Western Digital a zařízení nastavíme pro správné fungování na síti a také zvolíme metodiku pro ukládání dat RAID 1.

Obrázek 4.2-1



Na jednotlivé počítačové stanice nainstalujeme klientský software Synology Data Replicator 3, který zajistí přesouvání dat na NAS server. Každý uživatel bude mít na NAS serveru vyhraněnou složku, která bude zabezpečena pro jednotlivé uživatele uživatelským heslem a jménem. Tyto přístupové údaje nastavíme při nastavování klientského softwaru. Dále nastavíme na jednotlivých stanicích požadované složky, které vyžadují zálohu. Zálohování zvolíme v programu „Synchronizace“. To by mělo být provedeno tak, že se vytvoří úplná záloha a následně budou označené složky sledovány a v případě změny dat vytvoří kopii do NAS serveru. Tím bychom měli docílit nepřetržité ochrany stanic před

ztrátou dat. Pro obnovu dat využijeme rovněž klientský software, který se nainstauje na jednotlivé stanice. Program nabízí obnovu pomoci procházení dat, takže si můžeme zvolit danou verzi souboru, který chceme obnovit. Nebo můžeme zvolit obnovení pomoci hledání, kde nám program nabídne dle vyhledávacích požadavků verze souboru. Operaci obnovení by měl být schopný provést i zaměstnanec po proškolení administrátorem, jelikož je program v češtině a nabízí graficky intuitivní rozhraní. Měsíční periodu stanovím na přesunutí dat z NAS serveru na externí disk, který bude uschován u majitele firmy mimo budovy společnosti. Vlastní přesunutí by měl provést administrátor sítě. V případě poruchy NAS serveru bude nutné, aby administrátor tuto záležitost operativně řešil.

Cenová kalkulace

Náklady na vytvoření zálohovacího mechanismu rozepisuje tabulka 4.2-6. V této tabulce je veškerý potřebný hardware a odhadnutá cena instalace a nastavení tohoto hardware, kterou provede firma LWT JaryNet s.r.o. Náklady byly vyčísleny na 9 162,- Kč.

Tabulka 4.2-6

Položka	Množství	Cena za jednotku	Cena
Synology DS211j Disc Station	1	4 570,- Kč	4 570,- Kč
Western Digital Caviar Green WD5000AADS 3,5" 500GB	2	914,- Kč	1 828,- Kč
Samsung S2 Portable 500GB černý USB 3.0	1	1 544,- Kč	1 544,- Kč
TP-Link TL-SG1005D	1	420,- Kč	420,- Kč
Instalace a nastavení	-	800,- Kč	800,- Kč
Celkové náklady			9 162,- Kč

Při provozu bude vznikat náklad na správu zálohovacího mechanismu, kde bude nutné provádění kontroly a případné změny nastavení zálohování. Tento náklad byl odhadnut na 500,- Kč za měsíc, což představuje roční náklad 6 000,- Kč. Doporučuji, aby se o tuto správu starala firma LWT JaryNet s.r.o.

5 Zhodnocení navrhovaného řešení

Pro spojení dvou budov společnosti se hodí obě navrhovaná řešení. VPN varianta předčí svými možnostmi využití WiFi varianty. Navrhovaná VPN varianta poskytuje nejen spojení dvou sítí, ale také umožní napojení pracovníků společnosti do sítě skrz celosvětovou síť Internet odkudkoliv, kde budou mít k této sítí přístup a bude jejich počítač vhodně nastaven pro připojení k VPN routeru společnosti. Také v případě přemístění pracovníků do jiné budovy je znovu použitelná VPN varianta, kde postačí v nových prostorech napojení k internetu. Navrhované řešení za pomoci VPN tunelu je cenově méně nákladné na výstavbu než WiFi varianta. Provoz VPN varianty sice nevytváří viditelnou úsporu provozních nákladů po vytvoření spojení, ale nikterak nezvyšuje náklady na její údržbu. Náklady na vytvoření spojení mezi budovami jsou 3 765,- Kč. Tato cena však bude nepatrná při srovnání kolik práce navíc by bez tohoto řešení museli pracovníci z technické budovy vykonat, chtěli by pracovat s ekonomickým softwarem nebo jinými daty, které mohou být sdíleny při takto vytvořené síti.

Pro firemní data se snažím poskytnout maximální ochranu dat tak, že se nespoléhám pouze na jedno zařízení nebo jedno médium. Záloha se tak vytvoří na více zařízeních a nebude umístěna pouze v budově společnosti, ale data budou přenesena mimo ni. Pro takto vytvořenou zálohu navrhuji NAS server, na který budou kopírovány data z jednotlivých stanic, což vytvoří větší duplicitu dat a ochrání tato data před chybou dat jednotlivých stanic. Pro přesun dat z místa společnosti by měla být data přenesena na externím disku. Náklady pro vytvoření zálohovacího mechanismu jsou 9 162,- Kč. Cena navrhovaného řešení se může jevit jako příliš velká za bezpečnost dat. Při možné ztrátě dat by se tato cena vynaložená na zálohování jevila jako malá, při srovnání kolik si účtují různé společnosti za obnovu dat z poškozených medií. Přesto tyto firmy nedokážou mnohdy obnovit všechna data, proto je třeba předcházet ztrátě dat zálohováním.

U navrhovaných variant jsem dbal na objektivitu cen tím, že jsem využil pro dané řešení vždy jeden zdroj.

Celková cena navrhovaného řešení, která zahrnuje zálohovací mechanismus a spojení dvou budov v jednu síť vychází na 12 926,- Kč. Tím jsem splnil finanční kritérium pro vykonání řešení. Tyto jednorázové náklady na změnu sítě rozepisuje tabulka 5-1.

Tabulka 5-1

Položka	Náklad
Náklady na vybudovaní VPN spojení	3 765,- Kč
Náklady na vybudování zálohovacího mechanismu	9 162,- Kč
Celkové náklady	12 926,- Kč

Provozní náklady sítě se změní pouze v navýšení nákladů o správu sítě a správu zálohování. Ačkoli majitel firmy nechtěl, aby se náklady na provoz zvedly, navýšení ročních nákladů není markantní a je nevyhnutelné, chce-li si firma udržet ve správném chodu navrhnuté řešení. Kalkulace počítá se stejnou cenou za poskytování internetu. Navrhuji, aby společnost navázala spolupráci s firmou LWT JaryNet s.r.o., kterou jsem uvedl pro provedení změn v síti a vytvoření zálohovacího mechanismu, protože sídlí blízko a poskytuje služby pro vytvoření a správu navrhovaného řešení. Provozní náklady na chod sítě rozepisuje tabulka 5-2 s odhadovanými náklady na výjezdy pracovníků navrhované společnosti.

Tabulka 5-2

Položka	Roční náklad
Internet administrativní budovy	34 560,- Kč
Internet technické budovy	14 136,- Kč
Správa sítě	500,- Kč
Správa zálohovacího mechanismu	6 000,- Kč
Celkové roční náklady	55 196,- Kč

6 Závěr

Počítače a jejich sítě se staly nedílnou součástí firemních kultur s očekáváním usnadnění firemních úkolů, které plní zaměstnanci. V některých firmách tyto sítě a počítačové vybavení skrývají ještě nevyužité rezervy, v jiných je třeba něco doplnit, aby bylo možné splnit požadavek na usnadnění práce za pomoci využití informačních technologií.

Firma REZ servis s.r.o. požadovala rozšíření svého stávajícího počítačového vybavení z důvodu nedostatků jejich sítě a nedostačujícího zálohování dat. Cílem mé práce tedy bylo navrhnout vhodné spojení dvou vzdálených budov společnosti pro sdílení dat a navrhnout vhodný zálohovací mechanismus, který by ochránil data před možnou ztrátou nebo poškozením. Tyto cíle jsem si rozdělil na dva dílčí úkoly práce. Nejprve jsem v práci stanovil možné varianty propojení, a u dvou vhodných variant jsem stanovil vhodné prvky, které se nyní nabízí na trhu. Z těchto dvou vypracovaných variant, jak provést spojení, jsem vybral a doporučil výslednou variantu. U zálohovacího mechanismu jsem postupoval podobně. Vybral jsem vhodný postup, jak by měl mechanismus zálohování vypadat, a následně jsem provedl výběr vhodného hardwaru dostupného na trhu. Doporučením vhodných rozšíření sítě jsem splnil cíle práce.

Seznam použité literatury

[1] FOTR, J., *Manažerské rozhodování: postupy, metody a nástroje.* 1. vyd. Praha: Ekopress, 2006. 409s. ISBN 80-86929-15-9.

[2] HORÁK, J.; KERŠLÁGER, M. *Počítačové sítě pro začínající správce.* 4. vyd. Brno: Computer Press, 2008. 327s. ISBN 978-80-251-2073-6.

[3] KÁLLAY, F.; PENIAK, P. *Počítačové sítě LAN/MAN/WAN a jejich aplikace.* 2. vyd. Praha: Grada Publishing, 2003. 356 s. ISBN 80-247-0545-1.

[4] PUŽMANOVÁ, R. *Moderní komunikační sítě od A do Z.* 2. vyd. Brno: Computer Press, 2006. 430 s. ISBN 80-251-1278-0.

[5] TANENBAUM, A. *Computer network.* 2nd ed. Englewood Cliffs: Prentice Hall, 1989. 658 s. ISBN 0-13-166836-6.

[6] ZANDL, P. *Bezdrátové sítě WiFi: praktický průvodce.* 1. vyd. Brno: Computer Press, 2003. 190s. ISBN 80-7226-632-2.

[7] ZONKOVÁ, Z. *Rozhodování managera*. 1.vyd. Ostrava: VŠB-TUO, 1995. 94 s. ISBN 80-7078-254-4.

Internetové prameny

[8] MLEJNEK, M. Zálohování dat. SWMag.cz [online]. 2006-11-18 07 [cit. 2011-04-3]. Dostupné z WWW: < http://www.swmag.cz/150/zalohovani-dat/>.

[9] PUŽMANOVÁ, R. Virtuální privátní sítě pro vzdálený přístup. *DSL.cz* [online]. 2006-09-07 [cit. 2011-03-31]. Dostupné z WWW: <http://www.dsl.cz/clanek/511-virtualni-privatni-site-pro-vzdaleny-pristup>.

Seznam zkratek

UTP	Unshielded twisted pair
POE	Power over ethernet
GHz	Gigahertz
IPSec	Internet protocol security
MAC	Media access control
NAS	Network attached storage
PCMCIA	Peripheral komponent microchannel interconnect architecture
RAID	Redundant array of inexpensive/independent disks
SATA	Serial advanced technology attachment
USB	Universal serial bus
VPN	Virtual private network
WiFi	Wireless fidelity

Prohlášení o využití výsledků bakalářské práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 2.5.2011

……
Miroslav Rod

Adresa trvalého pobytu studenta:

Sv. Čecha 1093, Bohumín 735 81

Seznam příloh

Přílohy jsou přiloženy na CD.

Název	Formát	Cesta
D-Link_DNS-325	PDF	/NAS/
QNap_TS-210	PDF	/NAS/
Synology_DS211j	PDF	/NAS/
D-Link_DI-804HV	PDF	/VPN/
Mikrotik_rb750g	PDF	/VPN/
Zyxel_ZyWALL_5	PDF	/VPN/
AirLive_AirMax5	PDF	/WiFi/
Compex_WPP543A	PDF	/WiFi/
Kozumi_AirMax_5	PDF	/WiFi/
NanoBridge_M5	PDF	/WiFi/
Routerboard_sxt_5hnd	PDF	/WiFi/